

## ABSTRACT OF THE DISCLOSURE

A method of exchanging a cryptographic key between two users that includes the steps of selecting a value  $p$  from  $p=(2^{dk}-2^{ck}-1)/r$ ,  $p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\dots-2^k+1)/r$ ,  $p=(2^{dk}-2^{ck}-1)/r$ ,  $p=(2^{dk}-2^{ck}+1)/r$ , and  $p=(2^{4k}-2^{3k}+2^{2k}+1)/r$ ; selecting an elliptic curve  $E$  and an order  $q$ ; selecting a base point  $G$  on the elliptic curve  $E$ , where  $G$  is of order  $q$ ; generating a private key  $w$ ; generating a public key  $W=wG$ ; distributing  $p$ ,  $E$ ,  $q$ ,  $G$ , and  $W$  in an authentic manner; agreeing on  $p$ ,  $E$ ,  $q$ ,  $G$ ,  $W_1$ , and  $W_2$ , where  $W_1$  is the public key of a first user, and where  $W_2$  is the public key of a second users; each users generating a private integer; each users multiplying  $G$  by that user's private integer using a form of  $p$  agreed upon; each user transmitting the result of the last step to the other user; each users combining that user's private integer and public key with the other user's result of the tenth step and public key using the form of  $p$  agreed upon to form a common secret point between the users; and each user deriving the cryptographic key from the common secret point.